The invention claimed is:

1. A method comprising:

sending a control packet from a first endpoint of a tunnel through the tunnel to a second endpoint of the tunnel; and

waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets other than a control packet through the tunnel.

2. The method of claim 1 wherein the tunnel is a secure tunnel.

3. The method of claim 2 wherein the tunnel uses the IPSec security protocol suite.

4. The method of claim 3 wherein the tunnel uses ESP in tunnel mode.

5. The method of claim 1 wherein the tunnel traverses at least one network address translator (NAT).

6. The method of claim 5 wherein the first endpoint is a client and the second endpoint is a server.

7. The method of claim 5 wherein the NAT implements VPN Masquerade.

8. The method of claim 1 wherein the control packet is an ICMP echo request packet and the responsive control packet is an ICMP echo reply packet.

9. The method of claim 3 wherein the tunnel is defined by an epoch, the epoch comprising one security association (SA) in each direction, each SA having a negotiated limited lifetime and defining the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and with a security parameters index (SPI) chosen by the SA's destination.

10. The method of claim 9 wherein before the end of tunnel's lifetime the endpoints establish a new tunnel between them.

11. The method of claim 10 wherein a designated endpoint has responsibility for establishing the new tunnel and ignores requests initiated by the other endpoint to establish a new tunnel.

12. The method of claim 1 wherein the second endpoint waits for a packet from the first endpoint through the tunnel before using the tunnel to send any packets.

13. The method of claim 1 wherein if the first endpoint does not receive any packets through the tunnel for a predetermined time interval then the first endpoint sends through the tunnel a control packet to the second endpoint.

14. The method of claim 13 wherein if the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint.

15. The method of claim 10 wherein if an endpoint is unable to complete the establishment of a new tunnel before a predetermined time limit then that endpoint abandons establishment of that tunnel and starts establishing a new tunnel.

16. The method of claim 15 wherein if an endpoint successively fails to establish a new tunnel for more than a predetermined maximum number of times then that endpoint closes the connection currently being used to establish tunnels with the other endpoint and opens another such connection.

17. The method of claim 16 wherein the connection used to establish tunnels between the endpoints is an IKE session.

18. A computer readable media tangibly embodying a program of instructions executable by a computer to perform a method, the method comprising:

sending a control packet from a first endpoint of a tunnel through the tunnel to a second endpoint of the tunnel; and

waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets other than a control packet through the tunnel.

19. The computer readable media of claim 18 where in the method the tunnel is a secure tunnel.

20. The computer readable media of claim 19 where in the method the tunnel uses the IPSec security protocol suite.

21. The computer readable media of claim 20 where in the method the tunnel uses ESP in tunnel mode.

22. The computer readable media of claim 18 where in the method the tunnel traverses at least one network address translator (NAT).

23. The computer readable media of claim 22 where in the method the first endpoint is a client and the second endpoint is a server.

24. The computer readable media of claim 22 where in the method the NAT implements VPN Masquerade.

25. The computer readable media of claim 18 where in the method the control packet is an ICMP echo request packet and the responsive control packet is an ICMP echo reply packet.

26. The computer readable media of claim 20 where in the method the tunnel is defined by an epoch, the epoch comprising one security association (SA) in each direction, each SA having a negotiated limited lifetime and defining the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and with a security parameters index (SPI) chosen by the SA's destination.

27. The computer readable media of claim 26 where in the method before the end of tunnel's lifetime the endpoints establish a new tunnel between them.

28. The computer readable media of claim 27 where in the method a designated endpoint has responsibility for establishing the new tunnel and ignores requests initiated by the other endpoint to establish a new tunnel.

29. The computer readable media of claim 18 where in the method the second endpoint waits for a packet from the first endpoint through the tunnel before using the tunnel to send any packets.

30. The computer readable media of claim 18 where in the method if the first endpoint does not receive any packets through the tunnel for a predetermined time interval then the first endpoint sends through the tunnel a control packet to the second endpoint.

31. The computer readable media of claim 30 where in the method if the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint.

32. The computer readable media of claim 27 where in the method if an endpoint is unable to complete the establishment of a new tunnel before a predetermined time limit then that endpoint abandons establishment of that tunnel and starts establishing a new tunnel.

33. The computer readable media of claim 32 where in the method if an endpoint successively fails to establish a new tunnel for more than a predetermined maximum number of times then that endpoint closes the connection currently being used to establish tunnels with the other endpoint and opens another such connection.

34. The computer readable media of claim 33 where in the method the connection used to establish tunnels between the endpoints is an IKE session.